

Quand une analyse d'impact (AIPD) est-elle obligatoire au Luxembourg ?

Réponse courte

L'AIPD est **obligatoire** au Luxembourg dès qu'un traitement est susceptible d'engendrer un **risque élevé** pour les droits et libertés des personnes physiques, conformément à l'**article 35 du RGPD**. Trois cas sont expressément visés : l'**évaluation systématique et approfondie** d'aspects personnels fondée sur un traitement automatisé (profilage, scoring), le **traitement à grande échelle** de données sensibles ou relatives à des condamnations, et la **surveillance systématique** à grande échelle d'une zone accessible au public.

En outre, la **CNPD** publie une **liste de traitements** soumis à AIPD obligatoire : géolocalisation des salariés, dispositifs biométriques, vidéosurveillance des lieux de travail, traitements RH à grande échelle impliquant du profilage. La liste est régulièrement actualisée et doit être consultée avant tout nouveau traitement.

Définition

Le **risque élevé** s'apprécie en fonction de la **nature**, de la **portée**, du **contexte** et des **finalités** du traitement. Il résulte de la combinaison de la **probabilité** d'un impact négatif et de la **gravité** de cet impact pour les droits et libertés des personnes concernées, notamment en matière de vie privée, de discrimination, d'atteinte à la réputation ou de perte de contrôle sur les données.

Questions fréquentes

Dans quels cas l'AIPD est-elle obligatoire au Luxembourg ?

Trois cas sont expressément visés par l'article 35 du RGPD : évaluation systématique fondée sur traitement automatisé (profilage, scoring), traitement à grande échelle de données sensibles ou de condamnations, et surveillance systématique d'une zone accessible au public.

La géolocalisation des salariés impose-t-elle une AIPD ?

Oui, la géolocalisation (suivi GPS des véhicules ou smartphones professionnels) figure dans la liste publiée par la CNPD comme traitement soumis à AIPD obligatoire au Luxembourg, en raison de son caractère intrusif pour les salariés.

Qu'est-ce qu'un risque élevé au sens de l'AIPD ?

Le risque élevé s'apprécie en fonction de la nature, de la portée, du contexte et des finalités du traitement. Il combine la probabilité d'un impact négatif et la gravité de cet impact pour les droits et libertés des personnes concernées.

Qu'est-ce que la liste CNPD des traitements soumis à AIPD ?

La CNPD publie une liste de traitements soumis à AIPD obligatoire au Luxembourg : géolocalisation, biométrie, vidéosurveillance des lieux de travail, traitements RH à grande échelle. Cette liste est régulièrement actualisée et doit être consultée.

Que sont les neuf critères du CEPD pour l'AIPD ?

Les lignes directrices WP248 du CEPD énumèrent neuf critères (évaluation, décision automatisée, surveillance, données sensibles, grande échelle, croisement, vulnérabilité, nouvelle technologie, conséquences). Deux critères remplis suffisent en principe à rendre l'AIPD obligatoire.

Quelle sanction en cas d'absence d'AIPD obligatoire ?

L'absence d'AIPD lorsqu'elle est obligatoire est sanctionnée jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial. La CNPD peut également suspendre le traitement jusqu'à la réalisation de l'analyse d'impact requise.

Une vidéosurveillance des locaux nécessite-t-elle une AIPD ?

Oui, la surveillance systématique à grande échelle d'une zone accessible au public figure dans la liste de la CNPD comme nécessitant une AIPD. La vidéosurveillance des lieux de travail est un cas typique d'obligation d'analyse d'impact.

Conditions d'exercice

L'article 35 du RGPD rend l'AIPD obligatoire pour l'évaluation automatisée avec effets juridiques (scoring, profilage), le traitement à grande échelle de données sensibles, la surveillance systématique, la géolocalisation, la biométrie, et tout traitement figurant sur la liste publiée par la CNPD.

Cas visé	Exemple RH
Évaluation automatisée	Scoring de candidats, évaluation automatisée de performance
Données sensibles à grande échelle	Gestion d'un service de santé au travail important
Surveillance systématique	Vidéosurveillance de l'ensemble des locaux
Géolocalisation	Suivi GPS des véhicules ou smartphones professionnels
Biométrie	Contrôle d'accès par empreinte ou reconnaissance faciale
Profilage	Analyse prédictive des comportements des salariés
Nouvelle technologie	Déploiement d'outils d'IA ou d'analyse de données
Liste CNPD	Tout traitement figurant sur la liste publiée

Modalités pratiques

Selon les lignes directrices WP248 du CEPD, deux critères remplis parmi les neuf suffisent à rendre l'AIPD obligatoire, en complément de la liste publiée par la CNPD.

Étape	Détail
Description initiale	Cartographie du traitement envisagé
Check-list CNPD	Vérification par rapport à la liste publiée
Critères CEPD	Application des 9 critères des lignes directrices WP248
Décision documentée	Justification écrite de l'obligation ou de l'absence d'obligation
Avis du DPO	Consultation obligatoire avant lancement
Lancement AIPD	Méthodologie structurée si obligatoire
Consultation CNPD	En cas de risque résiduel élevé (art. 36)

Pratiques et recommandations

Consulter systématiquement la liste publiée par la CNPD avant tout nouveau traitement de données RH, pour identifier les obligations d'AIPD.

Appliquer les **neuf critères** du Comité européen de la protection des données (CEPD) : deux critères remplis suffisent en principe à rendre l'AIPD obligatoire.

Documenter la décision de mener ou non une AIPD, même lorsque l'obligation n'est pas retenue, pour démontrer l'analyse préalable.

Associer le DPO dès la phase d'analyse pour bénéficier de son avis formel sur la nécessité d'une AIPD.

Réviser la décision à chaque évolution du traitement ou de la liste de la CNPD, car un traitement initialement dispensé peut devenir soumis à AIPD.

Cadre juridique

Le cadre juridique de l'obligation d'AIPD repose sur le RGPD et les décisions de la CNPD.

Référence	Objet
Art. 35 RGPD	Obligation d'analyse d'impact
Art. 35.4 RGPD	Liste obligatoire publiée par l'autorité de contrôle
Art. 36 RGPD	Consultation préalable
Liste CNPD	Traitements soumis à AIPD au Luxembourg
Lignes directrices WP248	Critères du CEPD
Loi du 1er août 2018	Régime général au Luxembourg
Art. <u>L.261-1</u> Code du travail	Surveillance des salariés

L'**absence d'AIPD** lorsqu'elle est obligatoire est sanctionnée jusqu'à **10 millions d'euros ou 2 % du chiffre d'affaires mondial**. La CNPD peut également suspendre le traitement jusqu'à la réalisation de l'analyse.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.